

# PATENT COOPERATION TREATY

REC'D 07 NOV 2005

WIPO

PCT

From the  
INTERNATIONAL SEARCHING AUTHORITY

## PCT

### WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43bis.1)

To:  
PHILIP R. WADSWORTH  
QUALCOMM INCORPORATED  
5775 MOREHOUSE DRIVE  
SAN DIEGO, CA 92121

Date of mailing  
(day/month/year)

03 NOV 2005

Applicant's or agent's file reference

030457WO

FOR FURTHER ACTION

See paragraph 2 below

International application No.

PCT/US04/36284

International filing date (day/month/year)

28 October 2004 (28.10.2004)

Priority date (day/month/year)

29 October 2003 (29.10.2003)

International Patent Classification (IPC) or both national classification and IPC

IPC(7): H04L 9/00 and US Cl.: 713/176

Applicant

QUALCOMM INCORPORATED

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

#### 2. FURTHER ACTION

If a demand for international preliminary examination is made, this opinion will be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA/ US

Mail Stop PCT, Attn: ISA/US  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Facsimile No. (571) 273-8300

Date of completion of this opinion

17 October 2005 (17.10.2005)

Authorized officer

Joseph Pan

Telephone No. 571-272-5987

Form PCT/ISA/237 (cover sheet) (April 2005)

**WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY**

International application No.

PCT/US04/36284

**Box No. I Basis of this opinion**

1. With regard to the **language**, this opinion has been established on the basis of:

- ☐ the international application in the language in which it was filed
- ☐ a translation of the international application into \_\_\_\_\_, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b)).

2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:

a. type of material

- ☐ a sequence listing
- ☐ table(s) related to the sequence listing

b. format of material

- ☐ on paper
- ☐ in electronic form

c. time of filing/furnishing

- ☐ contained in the international application as filed.
- ☐ filed together with the international application in electronic form.
- ☐ furnished subsequently to this Authority for the purposes of search.

3. ☐ In addition, in the case that more than one version or copy of a sequence listing and/or table(s) relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

4. Additional comments:

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US04/36284

**Box No. V Reasoned statement under Rule 43 bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

|                               |                    |     |
|-------------------------------|--------------------|-----|
| Novelty (N)                   | Claims <u>1-45</u> | YES |
|                               | Claims <u>NONE</u> | NO  |
| Inventive step (IS)           | Claims <u>NONE</u> | YES |
|                               | Claims <u>1-45</u> | NO  |
| Industrial applicability (IA) | Claims <u>1-45</u> | YES |
|                               | Claims <u>NONE</u> | NO  |

2. Citations and explanations:

Please See Continuation Sheet

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US04/36284

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.

V. 2. Citations and Explanations:

Claims 1-45 lack inventive step under PCT article 33(3) as being obvious over Drews (U.S. Patent No. 6,477,645) in view of Bari et al. (U.S. Pub. No. 2002/0023059).

Drews discloses referring to FIG. 1, a block diagram of one embodiment of system 100 for providing authority and integrity checks in a system lacking a public key is shown. System 100 includes remote platform 105, user platform 110, including transformation value generator 115, comparison system 120, and display system 122. Remote platform 105 is coupled to user platform 110 by communication channel 125. User 130 is capable of receiving input, such as credential transformation value 135, information transformation value 140, or credential subset transformation value 145, from authorizing entity 150 for input into comparison system 120 of user platform 110. Remote platform 105 is capable of receiving information 155 and credential 160, which includes credential subset 165 from authorizing entity 150.

Remote platform 105 is capable, in one embodiment, of staging and transmitting information 155 and credential 160 to user platform 110. Remote platform 105 is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform 110 can function as remote platform 105.

The present invention ensures the authority and integrity of information received at user platform 110, so it is not limited in the type of information transmitted from remote platform 105 to user platform 110. In one embodiment of the invention, information 155 is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.

Credential 160, in one embodiment, contains authority information, such as a digital signature or digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential's digital signature installed on user platform 110, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.

User platform 110 is provided for the purpose of receiving transmitted information such as information 155, credential 160, or information 155 and credential 160 from remote platform 105. User platform 110 is the target device for software, commands, or data staged on remote platform 105, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform 105, user platform 110 is not limited to any particular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform 105 can be used in the present invention. (see column 2, lines 9-65 of Drews).

Transformation value generator 115 is provided to convert a variable length amount of digital data into a more concise form. In one embodiment of the invention, generator 115 is a hash function. A hash function accepts any length input and generates a fixed length output. Hash functions are known in the art and those skilled in the art will recognize that a hash

WRITTEN OPINION OF THE  
INTERNATIONAL SEARCHING AUTHORITY

International application No.  
PCT/US04/36284

**Supplemental Box**

In case the space in any of the preceding boxes is not sufficient.

function suitable for use in embodiments of the present invention is one that is relatively easy to compute, one-way, and collision-free. (see column 3, lines 15-23 of Drews).

In one embodiment, authorizing entity 150 supplies information transformation value 140, computed from information 155, to user 130. The transformation value is computed such that all parts of the information contribute to the transformation value in a way that is one-way and collision-free. In one embodiment, user platform 110 receives information transformation value 140 from user 130. Comparison system 120 compares the received information transformation value 140 with the output of transformation value generator 115, which generates a transformation value of information 155 supplied by remote platform 105. A match authenticates information 155 by ensuring the integrity and the authority of information 155. (see column 4, lines 24-37 of Drews).

Drews discloses the claimed subject matter. However, Drews does not specifically mention using the master credential in generating the application credential. On the other hand, Bari et al. disclose a system for registering, storing and managing personal data for use over a network, wherein the master credential is utilized (see paragraph [0046], lines 10-19 of Bari et al.). It would have been obvious to a person of ordinary skill in the art at the time the invention to utilize the master credential in generating the application credential. The ordinary skilled person would have been motivated to have applied the teaching of Bari et al. into method of Drew to utilize the master credential, because once a user is registered, the inventive system recognizes and authenticates the Master Authentication Credential, which then unlocks the personalized vault containing Authentication Master Credential for third party Web Sites and the User Profile (see paragraph [0036], lines 19-23 of Bari et al.).

Claims 1-45 meet the criteria set out in PCT Article 33(4), and thus have industrial applicability because the subject matter claimed can be made or used in industry.